

# 证 明

本证明之附件是向本局提交的下列专利申请副本

申 请 日： 2003 04 22

申 请 号： 03 1 23222.1

申 请 类 别： 发明

发明创造名称： 数字资源的分层密钥生成方法及其设备

申 请 人： 国际商业机器公司

发明人或设计人：张健；邵凌；裴云彰；谢东

中华人民共和国  
国家知识产权局局长

王 景 川

2004 年 1 月 30 日

# 权 利 要 求 书

1. 一种数字资源的分层密钥的生成方法, 包括:

5 将所述数字资源安排为至少一个树结构进行管理, 所述树结构的根节点代表数字资源的全集, 其它每个组节点分别代表数字资源的各级子集合, 最低一级为叶节点;

生成所述根节点的密钥; 以及

从所述根节点的密钥开始, 利用父节点的密钥按预定函数逐级计算其子节点的密钥, 直到叶节点为止。

10 2. 根据权利要求 1 所述的方法, 其特征在于: 即使两个节点具有相同的父节点, 计算所得的所述两个节点的密钥也不相同。

3. 根据权利要求 1 所述的方法, 其特征在于: 所述预定函数是单向函数。

15 4. 根据权利要求 1 所述的方法, 其特征在于: 采用随机的方式生成所述根节点的密钥。

5. 根据权利要求 1 所述的方法, 其特征在于还包括步骤: 直接或间接利用所计算出的节点的密钥加密相应的数字资源。

20 6. 根据权利要求 5 所述的方法, 其特征在于: 直接利用所生成的节点密钥的全部或部分或其变形形式加密对应的数字资源; 或先利用一密码加密所述数字资源, 再利用所生成的节点密钥的全部或部分或其变形形式加密所述密码, 其中所述变形形式是指对该节点密钥再演算的结果。

7. 根据权利要求 1 所述的方法, 其特征在于: 所述数字资源是视频、音频和文本资料中的至少一种。

8. 一种用于生成数字资源的分层密钥的设备, 包括:

25 密钥树管理装置, 用于将所述数字资源安排为至少一个树结构进行管理, 所述树结构的根节点代表数字资源的全集, 其它每个组节点分别代表数字资源的各级子集合, 最低一级为叶节点, 其特征在于, 所述设备还包括:

根节点密钥产生装置, 用于生成所述根节点的密钥; 和

30 计算装置, 用于从所述根节点的密钥开始, 利用父节点的密钥按预定函数逐级计算其子节点的密钥, 直到叶节点为止。

9. 根据权利要求 8 所述的设备, 其特征在于: 所述预定函数是单向函

数。

10. 根据权利要求 8 所述的设备, 其特征在于: 即使两个节点具有相同的父节点, 计算所得的所述两个节点的密钥也不相同。

5 11. 根据权利要求 8 所述的设备, 其特征在于: 所述设备还包括加密装置, 用于直接利用所生成的节点密钥的全部或部分或其变形形式加密对应的数字资源; 或先利用一密码加密所述数字资源, 再利用所生成的节点密钥的全部或部分或其变形形式加密所述密码, 其中所述变形形式是指对所述节点再演算的结果。

12. 一种用于管理数字资源的分层密钥的服务器设备, 包括:  
10 密钥树管理装置, 用于将所述数字资源安排为至少一个树结构进行管理, 所述树结构的根节点代表数字资源的全集, 其它每个组节点分别代表数字资源的各级子集合, 最低一级为叶节点, 其特征在于所述服务器设备还包括:

根节点密钥产生装置, 用于生成所述根节点的密钥;

15 第一计算装置, 用于从所述根节点的密钥开始, 利用父节点的密钥按预定函数逐级计算其子节点的密钥, 直到叶节点为止; 和

加密装置, 用于直接或间接利用所计算出的节点的密钥加密相应的数字资源。

20 13. 根据权利要求 12 所述的服务器设备, 其特征在于: 所述预定函数是单向函数。

14. 根据权利要求 12 所述的服务器设备, 其特征在于: 即使两个节点具有相同的父节点, 计算所得的所述两个节点的密钥也不相同。

25 15. 一种用于使用数字资源的分层密钥的客户机设备, 其中所述数字资源被安排为至少一个树结构进行管理, 所述树结构的根节点代表数字资源的全集, 其它每个组节点分别代表数字资源的各级子集合, 最低一级为叶节点, 其特征在于所述客户机设备包括:

第二计算装置, 用于根据从一服务器设备接收的节点密钥, 用预定函数依次计算出该节点的各个下级节点的密钥, 直到叶节点为止; 以及

30 解密装置, 用于使用已计算出的各个节点的密钥来解密该各个节点包含的数字资源。

16. 根据权利要求 15 所述的服务器设备, 其特征在于: 所述预定函数

是单向函数。

17. 根据权利要求 15 所述的服务器设备，其特征在于：即使两个节点具有相同的父节点，计算所得的所述两个节点的密钥也不相同。

## 数字资源的分层密钥生成方法及其设备

## 5 技术领域

本发明涉及一种数字资源的密钥管理方法，更具体地涉及一种数字资源的分层密钥生成方法。

## 背景技术

10 近年来，人们日常生活中的所有活动都趋于数字化，为了保护数字资源，广泛使用了具有加密技术的各种装置，也因此产生了对密钥进行管理的需要。由于要保护的数字资源的数量变得越来越庞大，如何安全地管理加密密钥成为更加突出的问题。

15 密钥管理包括下面三个基本特征：（1）密钥生成：为数字资源生成安全的加密密钥；（2）密钥存储：以安全的方式存储加密密钥；（3）密钥分配：将加密密钥传递给合法用户。

20 下面举出一个密钥管理的例子。假设在一个成熟可靠的电子教学系统中，所有的讲稿（教学资料）都应该用不同的密钥进行加密，并且已经为这些讲稿付费的所有合法用户都应该获得这些讲稿的加密密钥。在传统的方法中，密钥管理系统首先为每个讲稿生成密钥，然后将它们安全地存储在数据库

30 中，当一个用户为某些资源付费时，该密钥管理系统应该将该资源的相应密钥传递给该用户。

传统的密钥管理系统看起来好象工作得很好，但是当数字资源的数量爆炸性增长的时候，其成本会变得非常高。例如，如果在该电子教学系统中有 100,000 个讲稿，一个用户订购了其中的 20,000 个，并为这些讲稿付了费，那么就

25 就应该将这 20,000 个讲稿所对应的密钥安全地传递给用户。这里有两种可能的传递方法：（1）预先传递 20,000 个密钥；（2）在该用户需要的时候传递密钥。很显然，前者不够灵活，因为这些讲稿在以后的时间里可能被升级，也可能有一些附加的讲稿或组合在一起的讲稿，而这些变化不能在该用户已经得到的 20,000 个密钥中得到反映，即该用户可能得不到这些变化后的讲稿。相比较而言，后者虽然没有上述缺点，但是它却有成本非常高

10  
的缺点，因为为了获得这些密钥，仅仅该用户一个人就要进行 20,000 次请求。

近年来，在数字媒体的保护中主要存在两种密钥管理系统，即用于付费电视的条件访问（CA）系统和用于因特网的数字权利管理（DRM）系统。在  
5 CA 系统中，除了即看付费（pay-per-view）的节目外，一个月中的所有节目仅有一个密钥，这样，用户就不能仅仅订购单独一天甚至一个小时的节目，因此这个系统不够灵活。在 DRM 系统中，用户每次购买内容时，服务器都要检索内容的密钥，因此当用户和资源数量变得非常庞大的时候，服务器的负担就会变得很繁重。因此，上述 CA 和 DRM 系统的主要问题都在于密钥的  
10 存储和分配，而不是密钥的生成。

### 发明内容

为了解决上述 CA 系统和 DRM 系统中的问题，本发明的目的是提供一种数字资源的分层密钥生成方法。在本发明的分层密钥生成方法中，将所有的  
15 资源按照树结构进行管理，其中该树结构包括组节点和叶节点，每个组节点又包括根节点和非根节点的其它组节点，每个节点都对应着该数字资源中的不同的集合。每个上一级节点称为其下一级节点的父节点，而每个下一级节点称为其上一级节点的子节点。在本发明中，只随机地给出根节点的密钥，而其它节点的密钥都可以根据该节点的父节点的密钥利用单向函数计算得  
20 到。

因此，为了实现上述目的，本发明提供一种数字资源的分层密钥的生成方法，其中将所述数字资源安排为至少一个树结构进行管理，所述树结构的根节点代表数字资源的全集，其它每个组节点分别代表数字资源的各级子集合，最低一级为叶节点，其特征在于所述方法包括：生成所述根节点的密钥；  
25 以及从所述根节点的密钥开始，逐级利用父节点的密钥按预定函数计算其子节点的密钥，直到叶节点为止。

本发明还提供一种用于生成数字资源的分层密钥的设备，包括：密钥树管理装置，用于将所述数字资源安排为至少一个树结构进行管理，所述树结构的根节点代表数字资源的全集，其它每个组节点分别代表数字资源的各级子集合，最低一级为叶节点，其特征在于，所述设备还包括：根节点密钥产生装置，用于生成所述根节点的密钥；和计算装置，用于从所述根节点的密  
30

11  
钥开始，逐级利用父节点的密钥按预定函数计算其子节点的密钥，直到叶节点为止。

本发明还提供一种用于管理数字资源的分层密钥的服务器设备，包括：密钥树管理装置，用于将所述数字资源安排为至少一个树结构进行管理，所述树结构的根节点代表数字资源的全集，其它每个组节点分别代表数字资源的各级子集合，最低一级为叶节点，其特征在于所述服务器设备还包括：根节点密钥产生装置，用于生成所述根节点的密钥；第一计算装置，用于从所述根节点的密钥开始，逐级利用父节点的密钥按预定函数计算其子节点的密钥，直到叶节点为止；和加密装置，用于直接或间接利用所计算出的节点的密钥加密相应的数字资源。

本发明还提供一种用于使用数字资源的分层密钥的客户机设备，其中所述数字资源被安排为至少一个树结构进行管理，所述树结构的根节点代表数字资源的全集，其它每个组节点分别代表数字资源的各级子集合，最低一级为叶节点，其特征在于所述客户机设备包括：第二计算装置，用于根据从一服务器设备接收的节点密钥，用预定函数依次计算出该节点的各个下级节点的密钥，直到叶节点为止；以及解密装置，用于使用已计算出的各个叶节点的密钥来解密该各个叶节点包含的数字资源。

尽管本发明是一种密钥的生成方法，但是其也非常有利于密钥的存储和分配。根据本发明的方法生成的密钥数量大大减少，因此节省了进行密钥存储和分配所需要的大量成本，并且还具有足够的灵活性来支持资源的插入和删除等的变化。

### 附图说明

根据下面结合附图对本发明的具体实施例的详细描述，本发明的上述特点和优点将变得更加明显，其中：

图 1 是根据本发明对资源进行树结构管理的示意图。

图 2 是应用本发明的系统的示意图。

图 3 是示出根据本发明在服务器 1 中进行密钥管理的方法的流程图。

图 4 是示出根据本发明在客户机 2 中进行密钥管理的方法的流程图。

30

### 具体实施方式

下面将结合附图对本发明的具体实施方式进行详细地说明。

图 1 是根据本发明对电子教学系统中的资源进行树结构管理的示意图。

在图 1 的电子教学系统中，所有的讲稿都是数字化的，并被组织为树结构的各个课程。在本发明中，这些数字化的讲稿等都被称为数字资源。另外，该数字资源也可以是视频、音频和文本资料中的至少一种。其中，标记为 1 的节点是根节点，代表一种主课程，如数学、英语、和 MBA 课程等。标记为 2 的节点是非根组节点（也可以称其为子节点），各个非根组节点代表主课程下面的子课程，如在主课程节点“数学/”的下面再细分的节点“数学/几何/”、“数学/代数/”和在节点“数学/几何/”下再细分的节点“数学/几何/三角/”、“数学/几何/矩形/”等。根节点和非根的组节点都可以被称为组节点。而标记为 3 的节点是资源节点（也被称作叶节点，是该树结构中的最低一级），其包括各种课程中所具有的各个具体的讲稿，如资源节点“数学/几何/矩形/介绍”、“数学/几何/矩形/练习”、和“数学/几何/介绍”等。

为了将这些资源组织为树结构，需要三个基本的功能：（1）创建根节点，该根节点既可以是组节点，也可以是资源节点（即叶节点）；（2）在组节点下面创建下一级的组节点；（3）在组节点的下面创建资源节点。

另外，一个组节点可以有多级的次级节点，其中上一级的节点称为下一级节点的父节点，而下一级节点称为上一级节点的子节点。这些子节点既可以是组节点，也可以是资源节点。资源节点包括具体的数字资源（如讲稿），并且它不再具有子节点。从图 1 中可以看出，这个资源管理体系类似于一般的文件管理系统，但它可以有多个根节点。

如上所述的电子教学系统的密钥管理会变得非常容易。如果用户想要参加一个课程，他/她只需要简单地获得该课程的密钥，即某个组节点的密钥，而不需要获得该课程下面的各个子课程的所有密钥。如果该用户仅仅要订购三个讲稿，那么他/她就不需要订购整个课程，三个独立的讲稿密钥对于该用户来说已经足够了。

例如，在图 1 中，如果根节点“数学/”具有密钥  $K_1$ ，那么组节点“数学/几何/”将具有密钥  $K_2 = F(K_1, \text{“数学/几何/”})$ 。并且节点“数学/几何/矩形/”将具有密钥  $K_3 = F(K_2, \text{“数学/几何/矩形/”})$ 。最后的资源节点（即叶节点）“数学/几何/矩形/介绍”将具有密钥  $K_{4_1} = F(K_3, \text{“数学/几何/矩形/介绍”})$ 。同理，资源节点“数学/几何/矩形/练习”将具有密钥  $K_{4_2} = F(K_3,$

“数学/几何/矩形/练习”), 资源节点“数学/几何/矩形/问题解答”将具有  
密钥  $K4_3=F(K3, \text{“数学/几何/矩形/问题解答”})$ 。

例如, 在上述各个密钥中,  $K4_1$  或  $K4_1$  的一部分或对  $K4_1$  进行演算后所得  
的结果被用来加密资源节点“数学/几何/矩形/介绍”中的资源, 即与该节  
点相对应的讲稿。

当然, 也可以利用随机方法或其它方法为例如“数学/几何/矩形/介绍”  
的资源节点预先分配一个加密密钥, 然后再利用  $K4_1$  或  $K4_1$  的一部分或是对  $K4_1$   
进行演算后所得的结果来加密该预先分配的加密密钥。

在本发明的这个实施例中, 也可以在每个组节点的位置处存储相应的数  
字资源, 即讲稿, 从而如上所述地直接或间接地利用密钥  $K1$ 、 $K2$ 、 $K3$  或  $K4$   
来解密存储于相应节点位置处的数字资源。

这里,  $F()$  是单向函数, 表示一种算法, 该算法的逆算法是不可计算  
的。例如,  $y=F(x)$  非常容易计算, 而逆函数  $x=F^{-1}(y)$  基本上是不可能计算出  
来的。另外, 在本发明中, 单向函数  $F()$  可以由服务器侧提供给客户机侧,  
也可以不由服务器侧提供给客户机侧, 而是内嵌于客户机内。

很清楚, 如果用户具有密钥  $K1$ 、 $K2$ 、 $K3$  和  $K4$  (以下将资源节点密钥  $K4_1$ 、  
 $K4_2$ 、 $K4_3$  统称为  $K4$ ) 中的任何一个, 他/她都能解密该密钥所对应的节点的后  
代节点中所包含的资源 (即具体的讲稿)。一般情况下, 如果给定了一个  
组节点的密钥, 也就是实际上给出了该组节点的所有后代节点的密钥, 因为  
该用户可以从该节点的密钥计算出所有该节点的后代节点的密钥, 例如用户  
可以从节点密钥  $K3$  计算出其后代的各个资源节点的密钥  $K4_1$ 、 $K4_2$ 、 $K4_3$ 。这  
样, 如果向用户授权了一组资源, 只需要给他/她该组节点的密钥就足够了。

例如, 如果将组密钥  $K3$  分配给用户  $A$ , 那么用户  $A$  可以解密在该组节  
点“数学/几何/矩形/”以下的任何资源, 当然也包括将来经过变化 (如改  
变、增加或删除等) 的各个资源。例如即使现在系统中还没有资源“数学/  
几何/矩形/将来”, 但是只要该资源一出现在系统中, 用户  $A$  就可以解密该  
资源, 而无需分配给其额外的密钥, 这也为将来的密钥分配节省了大量的成  
本。

下面将结合图 2 说明应用本发明的系统。

图 2 是应用本发明的系统的示意图。

图 2 的系统可以是例如电子教学系统 (当然其它用途的系统也是可以

的)，包括相互连接起来的服务器 1 和客户机 2。当然，服务器 1 和客户机 2 也可以通过诸如因特网、企业网或局域网等的网络（未示出）相互连接。

服务器 1 除了包括一般的装置，如中央处理单元（CPU）、总线、存储器（ROM、RAM 等）（未示出）外，还包括密钥生成装置 19，用于产生所需要的各个密钥。所述密钥生成装置 19 包括根节点密钥产生装置 14，用于使用随机的方法或其它方法产生根节点的密钥；和第一计算装置 16，用于使用诸如单向函数的函数在该根节点密钥的基础上逐级计算该根节点的各个子节点的密钥，直到叶节点为止。同时，服务器 1 还包括加密装置 17，用于使用已计算出的密钥来加密相应节点中的资源，如教学讲稿等（另外，也可以利用随机方法或其它方法为例如“数学/几何/矩形/介绍”的资源节点预先分配一个加密密钥，然后再利用已计算出来的密钥的全部或一部分对该计算出的密钥进行演算后所得的结果来加密该预先分配的加密密钥）；以及密钥树管理装置 12，用于创建密钥的树结构（如前面结合图 1 所述的树结构），对创建出来的树结构进行维护，并对所计算出来的各个密钥进行存储和管理。

另外，服务器 1 还包括一第一通信端口（未示出），用于通过相应的连接线路或网络从客户机 2 接收请求和向客户机 2 发送被请求的内容和密钥等。

客户机 2 除了包括一般的装置，如中央处理单元（CPU）、总线、存储器（ROM、RAM 等）（未示出）外，还包括第二计算装置 26，用于使用从服务器 1 接收的、或其内部所嵌入的算法程序，在从服务器 1 接收的节点密钥的基础上逐级计算所需的各个子节点的密钥，以至最终计算出所需要的资源节点的密钥；和解密装置 27，用于使用已计算出的所述各个节点的密钥来解密所需要的资源，如教学讲稿等。

另外，客户机 2 还包括一第二通信端口（未示出），用于通过相应的连接线路或网络向服务器 1 发送请求，并从服务器 1 接收被请求的内容和密钥等。

当然，在上述服务器 1 和客户机 2 之间的通信中，经加密的资源以及客户机 2 所需要的节点密钥可以由服务器 1 同时传送给客户机 2，也可以分别进行传送。如在本发明中，服务器 1 只应客户机 2 的请求传送相应的节点密钥，被加密的资源等可以在其它时间、以其它任何方式传送给客户机 2，例如通过光盘等的方式将被加密的资源传递给客户机 2 等。

上述的第一和第二计算装置 16 和 26 可以通过在 CPU 上运行相应的软件程序来实现，也可以通过将一定的软件程序固化在诸如 CPU 的装置上而得到的硬件的形式来实现。另外，服务器 1 中的根节点密钥产生装置 14、第一计算装置 16 和加密装置 17 不限于上述的结构，也可以通过仅仅将它们的功能合并在一起的一个装置来实现。其中的根节点密钥产生装置 14 和第一计算装置 16 也不限于上述的结构，它们可以不包含在密钥产生装置 19 中，而是可以独立于密钥产生装置 19 之外。客户机 2 中的第二计算装置 26 和解密装置 27 不限于上述的结构，也可以通过仅仅将它们的功能合并在一起的一个装置来实现。

另外，上述各装置不限于仅分别包括在服务器 1 和客户机 2 中，也可以通过可操作的连接方式被置于服务器 1 或客户机 2 的外部。

下面将结合图 3 详细地说明本发明的密钥管理方法。

图 3 是示出根据本发明在服务器 1 中进行密钥管理的方法的流程图。

其中，在步骤 S100，由密钥树管理装置 12 创建各资源的树结构。可以根据资源的种类和大小创建多个树结构，如图 1 中所示。然后，处理过程前进到步骤 S104。

在步骤 S104，服务器 1 中的根节点密钥产生装置 14 产生资源树结构的根节点的密钥 K1，并将该密钥 K1 传送给第一计算装置 16。该根节点密钥 K1 可以是随机产生的，当然也可以用其它的方法来产生。

然后，在步骤 S106，第一计算装置 16 在所产生的根节点密钥 K1 的基础上，利用单向函数  $F()$  逐级地计算出各个子节点的密钥，直到资源节点（即叶节点）的密钥 K4 ( $K4_1$ 、 $K4_2$ 、 $K4_3$ ) 为止，并用所计算出的资源节点密钥 K4 或 K4 的一部分加密所对应的资源。具体地说，第一计算装置 16 先在所产生的根节点密钥的基础上，利用单向函数计算出该根节点的子节点（可能是一个组节点）的密钥，这里是组节点“数学/几何/”的密钥 K2，然后再在这个组节点密钥 K2 的基础上计算该组节点的子节点（可能是另一个组节点或资源节点）的密钥，这里是组节点“数学/几何/矩形/”的密钥 K3。这样一级一级地计算，直到计算出最后的资源节点密钥 K4（包括  $K4_1$ 、 $K4_2$ 、 $K4_3$ ）。

在计算出最后的资源节点的密钥 K4 后，服务器 1 用相应的节点密钥加密该各个节点所包括的资源。

在上述的计算过程中，所述计算各节点的密钥的计算程序可以相同，也可以不同。另外，即使各个节点具有相同的父节点，所得到的这些节点的各个密钥也是不相同的，例如资源节点“数学/几何/矩形/介绍”、“数学/几何/矩形/练习”和“数学/几何/矩形/问题解答”虽然具有相同的父节点“数学/几何/矩形/”，但是它们所分别具有的密钥  $K_{4_1}$ 、 $K_{4_2}$ 、 $K_{4_3}$  各不相同，这样就可以保证各个资源具有更高的安全性。

接下来，处理过程前进到步骤 S107。在步骤 S107，服务器 1 判断是否从客户机 2 接收到了对某些资源的请求。如果没有从客户机 2 接收到对特定资源的请求，则服务器 1 继续处于等待状态，直到从客户机 2 接收到请求。

10 如果在步骤 S107 中判断从客户机 2 接收到对某个资源的请求，例如是对节点“数学/几何/矩形/介绍”中的资源的请求，则处理过程前进到步骤 S108。

接下来，在步骤 S108，服务器 1 将客户机 2 所请求的相应节点的密钥传送给客户机 2。当然，同时也可以合并地、或单独地将客户机 2 所请求的经加密的资源传送给该客户机 2。

在完成步骤 S108 中的处理后，服务器 1 中的处理返回到步骤 S107 之前，处于等待状态，以等待接收下一个用户请求。

当然，在本发明的实施例中，在服务器 1 从客户机 2 接收到请求后，还可以包括一个认证过程，以检验发出请求的客户机 2 是否是其所请求资源的合法用户，例如，该客户机 2 是否已经为其所请求的资源付费等。

另外，在本发明的实施例中，服务器 1 在进行上述处理的过程中，还可以通过输入接口（未示出）从管理员处接受指令，并根据该管理员的指令对资源树的结构进行修改及对资源的内容进行增加/修改/删除等处理，并根据修改后的资源树结构进行重新生成根密钥、逐级计算各级密钥、加密修改后的资源内容等等的处理。

下面将结合图 4 描述本发明的密钥管理的方法在客户机 2 中的应用。

图 4 是示出根据本发明在客户机 2 中进行密钥管理的方法的流程图。

在图 4 中，在步骤 S200，客户机 2 经输入装置（未示出）从用户接收解密某个经加密的资源的请求，用来解密节点“数学/几何/矩形/”中的资源。接收到该请求后，客户机 2 在步骤 S202 检查本地的密钥库（未示出），以确定在本地的密钥库中是否存储有用来解密用户所请求的经加密的资源的

17  
密钥，例如是密钥 K3。在上述的密钥库中，存储有该客户机 2 以前从服务器 1 所接收的所有密钥。然后处理过程前进到步骤 S204。

在步骤 S204 中，客户机 2 判断在本地的密钥库中是否存储有用来解密节点“数学/几何/矩形/”中的资源的节点密钥 K3 或其各个上级节点的组密钥。

如果在步骤 S204 判断在客户机 2 的密钥库中存储有所请求节点资源的密钥 K3，则就用该本地存储的节点密钥 K3 解密相应节点“数学/几何/矩形/”的资源。另外，如果有必要，例如如果还需要资源节点密钥 K4，以解密节点“数学/几何/矩形/”的下级节点的资源，例如是资源节点“数学/几何/矩形/介绍”中的资源时，则第二计算装置 26 利用该本地存储的节点密钥 K3 计算出所需要的资源节点的密钥  $K4_1$ ，并使用资源节点密钥  $K4_1$  解密相应的资源。

如果在客户机 2 的密钥库中存储有包括所请求节点密钥 K3 的上级的组节点的密钥，例如可以是 K1 和 K2，则第二计算装置 26 利用该本地存储的组节点的密钥 K1 或 K2 逐级计算出所需要的资源节点的密钥 K3，以及需要的话还计算出资源节点的密钥  $K4_1$ ，并使用节点密钥 K3 以及资源节点密钥  $K4_1$  解密相应的资源。

如果在步骤 S204 中判断在客户机 2 的密钥库中没有所请求的组密钥或节点密钥 K3，则客户机 2 在步骤 S208 中向服务器 1 发出对密钥 K3 的请求。然后处理过程前进到步骤 S210。

在经服务器 1 验证该客户机 2 是合法用户后，在步骤 S210，客户机 2 从服务器 1 接收相应节点的密钥 K，密钥 K 可能是 K3，也可能是 K3 的上级组节点密钥，例如 K1 或 K2。

在步骤 S212，客户机 2 进行判断，判断所接收的密钥 K 是所请求的节点密钥还是其上级的组节点密钥。

如果判断是上级组节点的密钥（在本发明的实施例中判断为组节点“数学/几何/矩形/”的密钥 K3），则在步骤 S214，根据所接收的密钥 K3，利用客户机 2 内部所嵌入的算法程序，逐级地计算出被请求的资源所对应的各个资源节点的密钥，例如是  $K4_1$ 、 $K4_2$  或  $K4_3$ ，并用所计算出的资源节点的密钥  $K4_1$ 、 $K4_2$  或  $K4_3$  及所接收的节点密钥 K3 解密被请求的资源。上述逐级计算密钥的过程与服务器 1 中的步骤 S106 的过程相同，因此省略对其的详细描述。

如果在步骤 S212 判断所接收的密钥是所请求的资源节点密钥，例如当客户机 2 请求解密资源节点“数学/几何/矩形/介绍”时，其从服务器 1 接收的节点密钥是  $K4_1$ ，则处理前进到步骤 S216。在步骤 S216，客户机 2 确定所接收的节点密钥是所请求的资源节点的密钥  $K4_1$ ，因此，客户机 2 不再进行逐级地计算，而直接利用所接收的资源节点的密钥  $K4_1$  解密所得到的、经过加密的资源。

在上述判断所接收到的节点密钥是对应于哪一个节点密钥的过程中，可以利用服务器 1 在产生该密钥时对该密钥所加入的标识符来进行，当然也可以通过本领域的技术人员所熟悉的其它方式来进行。

本发明上述产生根节点密钥的方法也可以是这样的，即服务器 1 不是在接到客户机 2 的请求前预先存储了相应根节点的密钥及逐级计算出来的各级密钥，而是在接到客户机 2 的请求后才产生某个根节点的密钥，然后再逐级计算出各级密钥。

通过上述的描述可知，由于在本发明的方法中，服务器 1 在接收到来自客户机 2 的请求前只存储根节点的密钥就已经足够了，或根本无须存储各个密钥，所以本发明的方法将减少对资源密钥的存储要求。并且密钥的分配也得到简化：假设一个用户被授权使用 20,000 个资源，他/她只需要获得几个（例如可以是 20 个）组节点密钥就可以了，而无需获得 20,000 个密钥。这样就大大减少了在网络上传送密钥所需要的大量带宽，节省了进行密钥存储和分配所需要的大量成本。

上面对本发明的实施例进行了详细地描述。本领域的普通技术人员应该明白，按照本发明的精神及指导思想对本发明做出的各种修改都在本发明后附的权利要求书所要求保护的范围内。

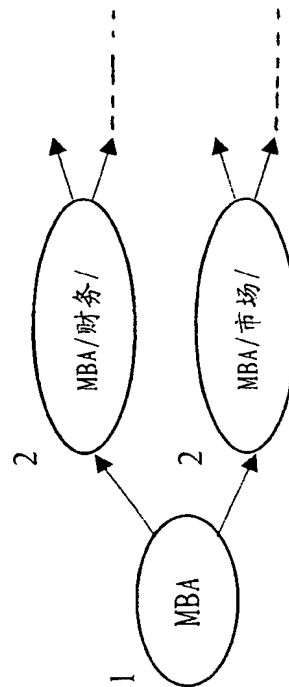
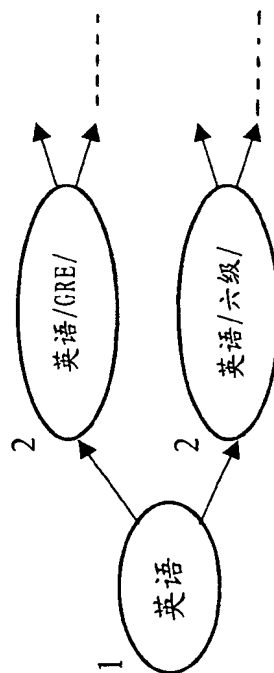
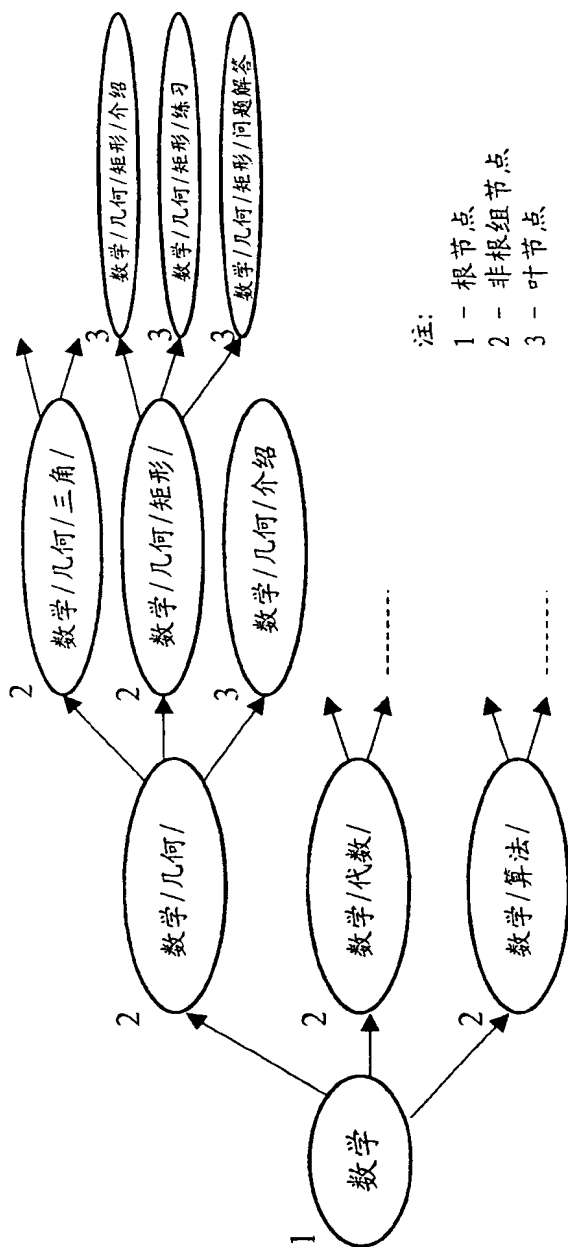


图 1

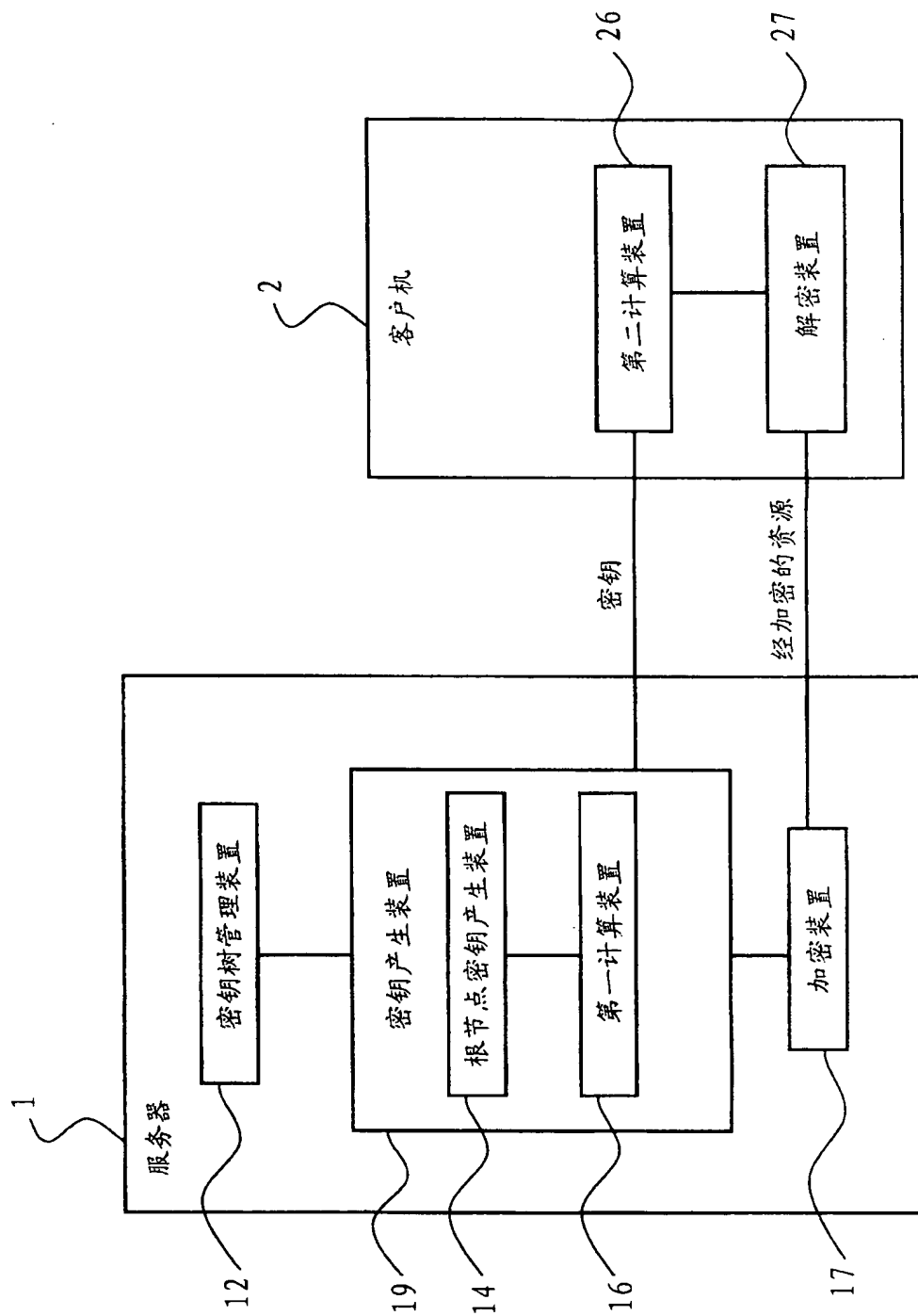


图 2

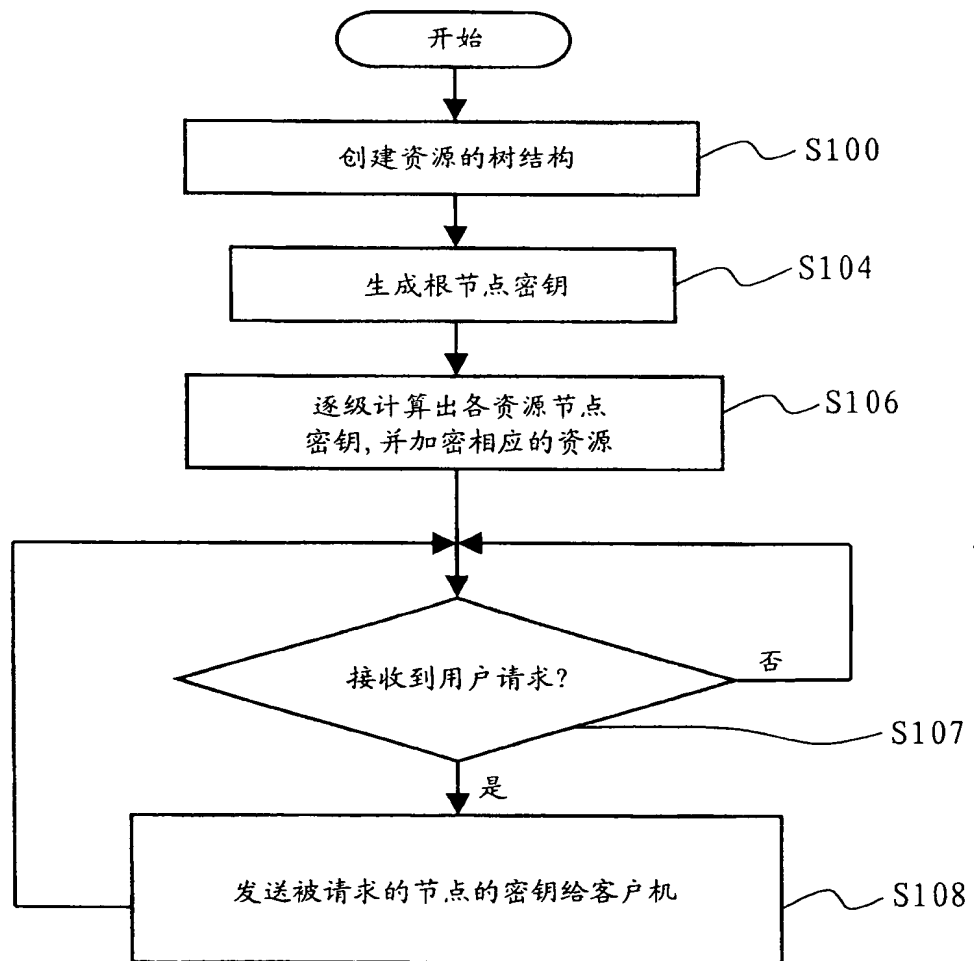


图 3

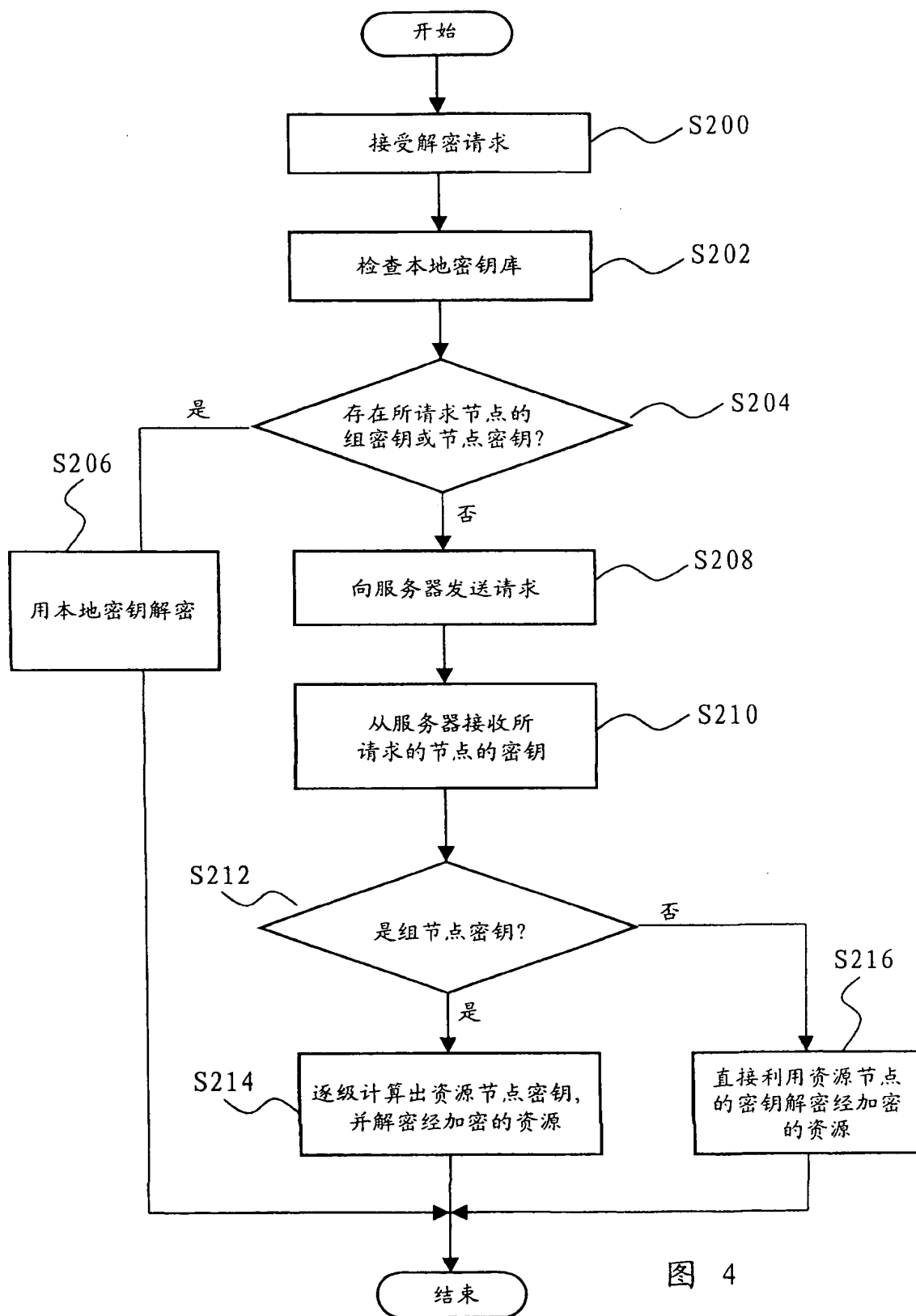


图 4